ELSEVIER

Signal Processing: *Image Communication* 16 (2001) 681–699

SIGNAL PROCESSING:
IMAGE
COMMUNICATION

www.elsevier.nl/locate/image

An overview of multimedia content protection in consumer electronics devices

Ahmet M. Eskicioglu[a,*], Edward J. Delp[b,1]

[a] *Thomson Consumer Electronics, Corporate Research, 101 W. 103rd Street, Indianapolis, IN 46290-1102, USA*
[b] *Video and Image Processing Laboratory (VIPER), School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907-1285, USA*

Received 15 March 2000; accepted 10 August 2000

Abstract

A digital home network is a cluster of digital audio/visual (A/V) devices including set-top boxes, TVs, VCRs, DVD players, and general-purpose computing devices such as personal computers. The network may receive copyrighted digital multimedia content from a number of sources. This content may be broadcast via satellite or terrestrial systems, transmitted by cable operators, or made available as prepackaged media (e.g., a digital tape or a digital video disc). Before releasing their content for distribution, the content owners may require protection by specifying access conditions. Once the content is delivered to the consumer, it moves across the home network until it reaches its destination where it is stored or displayed. A copy protection system is needed to prevent unauthorized access to bit streams in transmission from one A/V device to another or while it is in storage on magnetic or optical media. Recently, two fundamental groups of technologies, encryption and watermarking, have been identified for protecting copyrighted digital multimedia content. This paper is an overview of the work done for protecting content owners' investment in intellectual property. © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Multimedia; Copy protection; Cryptography; Watermarking; Consumer electronics; Digital television; Digital video disc; Digital video cassette; Home networks

1. Introduction

In the entertainment world, original multimedia content (e.g., text, audio, video and still images) is made available for consumers through a variety of channels. Modern distribution systems allow the delivery of content to millions of households every day. Although legal institutions exist for protecting intellectual property (trademarks and patents) owned by content creators, complimentary technical measures are needed to sustain financial returns and to ensure incentives for new creations.

In order to see the increasing importance of protecting copyrighted content, one should understand an essential difference between old and new technologies for distribution and storage. Prior to the development of digital technologies, content was created, distributed, stored and displayed by analog means. The popular video cassette recorders

[*] Corresponding author.
E-mail addresses: eskicioglua@tce.com (A.M. Eskicioglu), ace@ecn.purdue.edu (E.J. Delp).

[1] Portions of this work done by EJD were supported by the sponsors of the Center for Education and Research in Information Assurance and Security at Purdue University.

0923-5965/01/$ - see front matter © 2001 Elsevier Science B.V. All rights reserved.
PII: S0923-5965(00)00050-3

(VCRs) of the 1980s introduced a revolutionary way of viewing A/V content, but ironically allowed unauthorized copying, risking the investments made in intellectual property. An inherent characteristics of analog recording, however, prevented piracy efforts to reach alarming proportions. If a taped content is copied on a VCR, the visual quality of the new, i.e., the first-generation, copy is reduced. Further generational copies result in noticeably less quality, decreasing the commercial value of the content. Today, reasonably efficient analog copy protection methods exist, and have recently been made mandatory, in consumer electronics devices to further discourage illegal analog copying. An example of such a system was developed by Macrovision[2] whereby features of the analog composite video signal are modified to prevent copying.

With the advent of digital technologies, new tools have emerged for making perfect copies of the original content. A quick review of digital representation of data will reveal why generational copies do not lose their quality. A text, an image or a video is represented as a stream of bits (0s and 1s). This representation can be conveniently stored on magnetic or optical media. Since digital recording is a process whereby each bit in the source stream is read and copied to the new medium, an exact replica of the content is obtained. Such a capability becomes even more threatening with the ever increasing availability of Internet, an immense and boundless digital distribution mechanism. Protection of digital multimedia content therefore appears to be a new and crucial problem for which immediate solutions are needed.

Three major industries have a great interest in this problem:

1. motion picture industry,
2. consumer electronics (CE) industry,
3. information technology (IT) industry.

The content owners are the motion picture studios. Their content (movies) is displayed or recorded on devices manufactured by consumer electronics companies. The information technology industry manufactures general purpose computing devices, such as personal computers, which can also be used to display and store content.

Research conducted by the CE and IT industries has revealed two promising groups of technologies. Encryption-based technologies transform content into unintelligible or unviewable form. This transformation, being reversible in nature, allows perfect recovery of content. Both symmetric and public key ciphers are commonly used for content security and authentication (see Section 4). Technologies based on watermarking serve several purposes: identification of the content origin, tracing illegal copies and disabling unauthorized access to content.

This paper highlights recent developments in protecting copyrighted multimedia content. The exact details of the copy protection systems will be omitted throughout the presentation due to security issues and for the protection of intellectual property.

2. What is the copy protection problem?

2.1. Problem definition and possible approaches

The home network depicted in Fig. 1 may receive content from a variety of sources, including cable operators, satellite or terrestrial broadcasters, and telephony centers. Pre-recorded media is also considered to be a content source. A commonality of all these sources is that they protect the content in some private way before delivery. Examples are the protection provided by the DirecTV Digital Satellite System (DSS) system and the Content Scramble System (CSS) for DVDs. When the scrambled content reaches the "boundaries" of the network, an authorized "access device" (a DSS set-top box or a DVD player) descrambles the stream, and makes it available for display or storage. The content then has to be sent to a display or storage device.

A global copy protection framework needs to address two problems: protection of content in transmission and protection of content in storage. Copy protection technologies offer methods and tools to prevent unauthorized access. The approaches used in deploying these technologies can fit into two broad categories:

[2] http://www.macrovision.com/

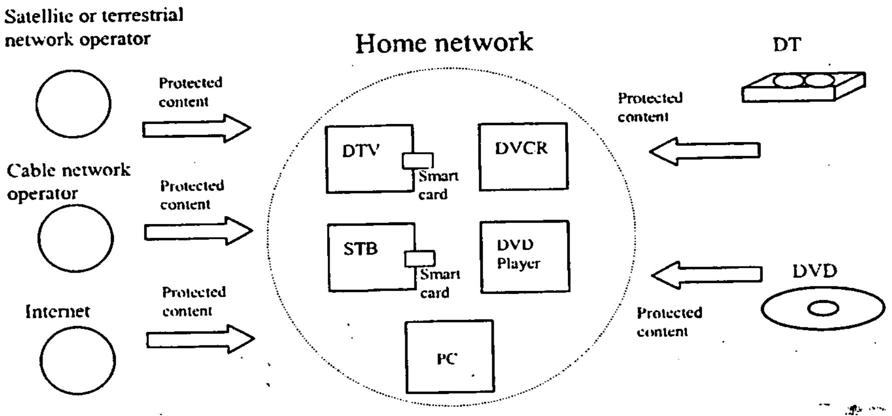

Fig. 1. Sources of content for home networks.

With feedback provided by the content owners, the CE and IT industries have been developing solutions in specific areas. The CSS, for example, provides protection for content recorded on DVD-ROM discs (see Section 7). Other systems are proposed for securing the IEEE 1394 interface, and preventing unauthorized copies on recordable DVDs (DVD-R/RW/RAM).

An alternative approach is to develop global architectures based on removable security devices. Such architectures are considered extensions of conditional access systems, restricting viewing when the consumer does not have the correct entitlements (see Section 10). The National Renewable Security Standard (NRSS) provides a means for separating the security functionality from navigational devices (see Section 9).

The recording industry is another major player in the copy protection arena who has chosen a separate path to develop a solution for musical content. The recent launch of the Secure Digital Music Initiative (SDMI) is an indication of the strong need for secure distribution of music (see Section 11).

2.2. Various types of attacks

It is important to keep in mind what attacks are supposed to be prevented in a copy protection system. Generally, the following categories of attack are discussed:

- Commercial piracy: a commercial entity steals content, makes a master, and begins making and selling illegitimate copies. None of the copy protection systems discussed in this paper help with this problem. Commercial entities that can create a manufacturing facility will always be able to get to a clear bitstream, or simply to duplicate a pre-recorded content. The key to fighting this type of piracy is tracing the source of the illegitimate content and taking legal action. Watermarking may be of best use here.
- "Garage" piracy: an individual with smaller resources makes a few dozen or hundred illegitimate copies and sells or barters them. It is also probably true that none of the copy protection systems can defeat this pirate. A "garage" pirate, skilled in engineering, will be able to take apart his TV/VCR/STB, and probe a PC board for a clear bitstream (which is present in all current products, and will be for several years). However, a useful deterrent is to void instrument the warranty if it is so modified. This will discourage most of the population. Once again, legal means are probably the only way to fight this type of piracy, and watermarks may turn out to be helpful as a tracing tool.
- "Ant" piracy: an individual wants to make a few copies of something for his friends, relatives, or even for his own use. In general, this person will

have very limited resources, and will not be skilled in engineering. Ant piracy is prevented by the copy protection systems shown here.

2.3. *Design factors*

All security systems based on encryption and watermarking are bound to be broken in time given sufficient resources. Hence, a number of important factors need to be taken into consideration in designing systems for protecting content in CE devices. These include robustness, renewability and cost.

Robustness: Refers to how strong the system is against conceivable attacks. Every successful design should produce a security system that is sufficiently robust for the application it is used for.

Renewability: When a protection system is hacked, there must be a way to replace it with a new, more robust system. This general concept can be implemented in two fundamental ways. (1) Replacement of renewable security device: all the security functionality is assigned to a renewable device such a smartcard. When its secrets are disclosed, it is simply replaced by a new card. (2) Revocation of CE device: the secrets are embedded in the CE device, and cannot be removed. If the device is understood to be a pirate device, it is not allowed to receive copy-protected content.

Cost: The CE industry is in a constant effort to minimize the cost of manufacturing so that the end product is affordable for the consumer. Any additional cost needs to be justified from the consumer's viewpoint.

There is a critical balance between the robustness and cost of copy protection systems. A system should neither be too expensive nor easily hackable. Ideally, every security system needs to be renewable to minimize the damage caused by a system hack. However, the transition to the new system should be transparent to the customer.

3. WIPO and digital millennium copyright act

The World Intellectual Property Organization (WIPO) is an intergovernmental United Nations organization with headquarters in Geneva, Switzerland. It is responsible for the promotion of the protection of intellectual property throughout the world through cooperation among States, and the administration of various multilateral treaties dealing with the legal and administrative aspects of intellectual property.

Intellectual property comprises two main branches:

- Industrial property: chiefly in inventions, trademarks, industrial designs, and appellations of origin.
- Copyright: chiefly in literary, musical, artistic, photographic and audiovisual works.

The number of member States as of 15 April 1999 was 171. Members include Switzerland, member states of the European Union, USA, China and others.

WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty were adopted by a WIPO conference in Geneva on 20 December 1996 based on existing international treaties (the Berne Convention for the Protection of Literary and Artistic Works as revised in Paris on 24 July 1971, and the Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations of 26 October 1961). Before becoming binding law in the member states, the provisions of the treaties have to be ratified by the member States and national legislation has to be amended. It is not mandatory for WIPO Member States to ratify the treaties; however, the most important Contracting Parties, among them the USA, were expected to do so.

The Digital Millennium Copyright Act (DMCA) [11] was prepared to amend title 17, United States Code, to implement the WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty, and for other purposes. It includes five titles:

- WIPO Treaties Implementation,
- Online Copyright Infringement Liability Limitation,
- Computer Maintenance or Repair Copyright Exemption,
- Miscellaneous Provisions,
- Protection of Certain Original Designs.

How the DMCA will be used to enforce copy protection is an open question. The movie industry used the DMCA to sue individuals who attacked the Content Scramble System (CSS) system. With regard to watermarking, the applicability of the DMCA may not be obvious. It is widely believed that if one attempts to deliberately remove or attack a watermark then this a violation of the DMCA. However, does the DMCA require that a watermark has to be detected if one is present in the content?

4. Basic concepts and definitions in cryptography and watermarking

To have a better understanding of the impact of protection methods on consumer electronics devices, we will start with a summary of basic concepts and definitions in cryptography and watermarking.

4.1. *Cryptography*

Cryptography [7,8,23,25,29] deals with the concealment and protection of digital information. The study of cryptographic techniques is more than 400 years old. Shannon's 1949 paper [30] that connected cryptographic techniques with digital communication theory is thought by many to be the beginning of "modern" cryptography [20].

A cryptographic system consists of five elements: a plaintext message space, a ciphertext message space, a key space, a family of enciphering transformations, and a family of deciphering transformations. In modern cryptosystems, the enciphering and deciphering transformations are public, only the keys need to be kept secret. Cryptanalysis is the science and study of "breaking" or attacking ciphers.

Ciphers can be classified according to two important criteria: (1) symmetric versus asymmetric and (2) stream versus block.

In a symmetric key cipher, enciphering and deciphering keys are the same or can easily be determined from each other. Asymmetric key systems (public key systems) differ in such a way that at least one key is computationally infeasible to determine from the other. The key used for encryption is publicly available, while the corresponding decryption key should be kept confidential all the time [9,10].

A stream cipher breaks the message M into successive characters or bits $m_1, m_2, m_3, \ldots$, and enciphers each m_i with the ith element k_i of a key stream $K = k_1k_2k_3, \ldots$ A block cipher breaks the message M into successive blocks $M_1, M_2, M_3, \ldots$, and enciphers each M_i with the same key K.

An example of symmetric and asymmetric key ciphers is shown is Fig. 2. When the two parties A and B want to communicate securely, each approach introduces key management problems. In case (a), both parties need to have a copy of the symmetric key, the distribution of which is a non-trivial problem. The problem with case (b) is the authentication of the public key that is used for encryption; A needs assurance that it has the public key that actually belongs to B.

Using public key cryptographic techniques, one can provide assurance about the integrity or reliability of a public key or other types of data. This is usually referred to as authentication [29]. There are two types of authentication protocols. In message authentication, a party is corroborated as the original source of specified data created at some time in the past. In entity authentication, one party is assured of the identity of a second party involved in a protocol, and that the second party has actually participated.

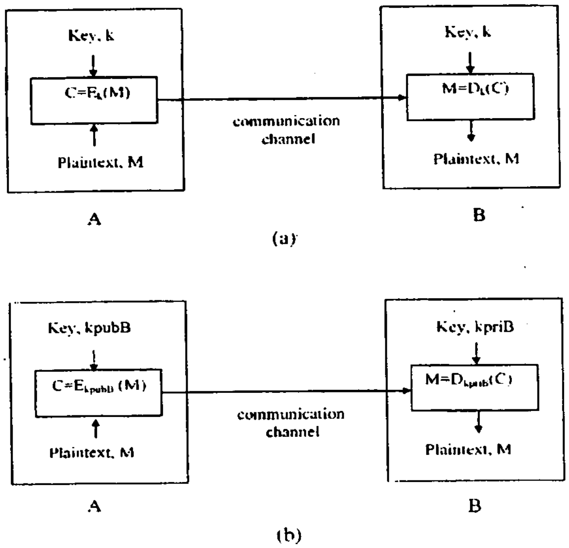

Fig. 2. Encryption: (a) symmetric key, (b) asymmetric key.

A digital signature [29], which associates a message with some originating entity, can be constructed with public key systems. Each digital signature scheme includes a signature generation algorithm and a signature verification algorithm. A public key certificate [23] is a digitally signed message consisting of two parts which can be used to authenticate a public key. The "data part" includes the public key that is being authenticated, as well as other information such as the issuer, the owner, and the validity period of the public key. The "signature part" is the signature on the data part generated by the issuer of the certificate.

4.2. *Watermarking*

Watermarking [24,31] is the process of embedding data (or controlled distortion) into a multimedia element such as image, audio and video. This embedded information, known as the watermark, can later be extracted from the multimedia and used for security purposes [19]. In multimedia applications, the watermark should be invisible or inaudible to the human observer (visible watermarking techniques do exist) [33]. A watermarking algorithm consists of the watermark structure, an embedding algorithm and an extraction or detection algorithm. Watermarks can be embedded into multimedia directly (e.g., the time domain) or after the multimedia element has been transformed (e.g., the discrete cosine transform) [6]. Performance issues include robustness to attack (attempts to remove the watermark), capacity (how bits can be hidden in the multimedia) and how transparent is the watermark under normal viewing or listening conditions. There has been a tremendous amount of work done in watermarking in the past 6 years [24].

Typical uses of watermarks include identification of the origin of content, tracing illegally distributed copies, and disabling unauthorized access to content. A mature robust watermarking technology should be resistant to many types of attacks and normal A/V processes such as noise, filtering, resampling, cropping, data compression, and A-to-D and D-to-A conversions.

There is an important difference between encryption and watermarking in enforcing protection. With an encryption-based technology, it is possible to protect content (video or audio) because licensing allows the implementer to have access to the keys. If keys are not available, content cannot be accessed. Watermarks do not preclude access to the watermarked content. The receiving device needs to have the detection capability. Thus, a legal mechanism is needed to enforce the manufacturers to implement detectors in devices. In the US, no such legislation is expected in the future. Nevertheless, hybrid technologies with encryption and watermarking may address this limitation through licensing.

4.3. *Multilayer protection by encryption and watermarking*

Encryption or watermark based technologies can be independently used for protecting multimedia content. However, it is possible to implement both in the same application, providing a two-layer protection. As shown in Fig. 3, the content may

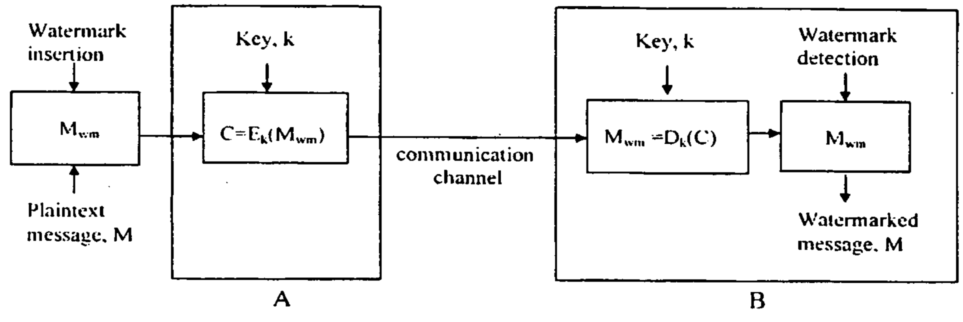

Fig. 3. Two-layer protection.

have been watermarked immediately after creation. The sending party encrypts the watermarked content to provide the second layer of protection. At the receiving end, the stream is decrypted before watermark detection takes place.

5. The beginnings

The work on copy protection started almost four years ago. At the beginning of 1996, a bill was drafted as a result of collaboration between consumer electronics companies and content owners. The "Video Home Recording Act of 1996" was intended to amend title 17, United States Code, to "*govern the importation, manufacture and distribution of digital motion picture recording and related services, to prohibit certain copyrighted infringement actions, and for other purposes*". One section of the Act was a technical reference document for establishing the standards and specifications for implementing technological management of consumer copying of linear motion pictures. Before the bill was actually submitted to the US Congress, the three industries (CE, IT and motion picture) wanted to resolve all outstanding issues, and agreed to create a forum for discussion.

The forum gave birth to a plenary group which was comprised of both technical and policy representatives of the member companies of the MPAA,[3] CEMA,[4] BSA,[5] ITIC[6] and RIAA[7]. Each expertise group (technical and policy) was assigned a specific task that was completed in late June of 1996. The findings were presented in two reports on 21 June 1996. The report of the policy group summarized the exploratory discussions regarding the concepts of anti-circumvention in conjunction with the introduction of digital video technologies, and the key policy considerations to be weighed in making decisions about specific technical and legislative proposals. Focusing on technical issues, the other group identified and evaluated the technical approaches to protect content in analog or digital form, delivered by direct electronic transmission or prerecorded media. After these presentations, the technical group, now known as the Copy Protection Technical Working Group [2] (CPTWG), continued discussing copy protection problems. It is still active today, having monthly meetings to discuss the current issues.

In the past three years, CPTWG formed working groups to focus on specific problems [3]. Two of the most active groups were the Digital Transmission Discussion Group (DTDG) and the Data Hiding Subgroup (DHSG).

The DTDG was created on 3 October 1996. Its scope was to define a data protection system (DPS) that can be used to protect digital audio/video transmitted on the IEEE 1394 high performance serial bus [32]. The architecture developed for DPS had three layers:

1. Copy Control Information (CCI) Layer – a means of carrying information along with the copyrighted content that expresses the intentions of the copyright holder with regard to the conditions under which an end consumer is authorized to make a copy.
2. Device Authentication and Key Exchange Layer – a means of a compliant device to establish the authenticity of another device prior to exchanging copyrighted content, and also to generate the keys for data encryption.
3. Data Encryption Layer – a means of encrypting the copyrighted content when it is transmitted from one compliant device to another compliant device in digital form.

The DTDG issued a Call for Proposals on 11 March 1997, and published its "Review and Findings" report [27] summarizing the technical features of the submitted proposals. After completing its task, the DTDG closed in February 1998. Five of the proposals included in the DTDG report later merged to form the 5C group [4].

The DHSG was created on 6 May 1997. Its scope was to define a data hiding system that can be used to mark video content for the purposes

[3] Motion Picture Association of America (http://www.mpaa.org).

[4] Consumer Electronics Manufacturing Association (now known as the Consumer Electronics Association, http://www.ce.org).

[5] Business Software Alliance (http://www.bsa.org).

[6] Information Technology Industry Council (http://www.itic.org).

[7] Recording Industry Association of America (http://www.riaa.org/).

of identifying marked material and preventing unauthorized recording/playback. The Call for Proposals issued on 1 July 1997 identified a set of essential and desirable requirements for the system. The Interim Report [21] published by DHSG included the performance of seven proposals during visibility and survivability tests.

Because of prolonged discussions, the "Video Home Recording Act of 1996" could not be submitted to the US Congress.

6. Desirable attributes for a copy protection system

The first step in developing a system in any field of engineering is to determine the system requirements. Although work on copy protection had been continuing for some time, a list of desirable attributes applicable to a copy protection system was not available until recently. Recognizing the need, CEMA put together a list, and presented it to the MPAA. Instead of providing feedback to CEMA's work, the MPAA chose to publish its own list. Ironically, both lists were created long after the development of some of the copy protection systems.

6.1. CEMA list

The attributes are presented in three groups:

General

1. Offers a sufficient level of security to "keep honest people honest".
2. Is likely to achieve broad multi-industry consensus and receive support of industries participating in the CPTWG.

Technical

3. Is renewable.
4. Is applicable to one or more of the following four interfaces: IEEE 1394, RF Remodulator (Section 9), NRSS A&B (Section 9), and Component Video.
5. Has low complexity in implementation, operation, maintenance and administration.
6. Provides transmission and storage protection.
7. Does not result in perceptible degradation of content.
8. Does not inhibit desirable and currently available features on CE products such as trick play.
9. Is extendable to general-purpose computing architectures, allowing interoperability of CE and general-purpose computing devices.
10. Has components available competitively from as large a number of sources as possible.

Consumer

11. Allows time shifting of transmitted content (i.e., recording) for fair use.
12. Allows place shifting of content (e.g., the ability to play a lawfully made recording at a friend's house on compliant equipment).
13. Allows free copying of content, including over-the-air and non-premium services, accommodates generational control of premium services, and permits the copyright owner to prevent copying of pay-per-view and video-on-demand services as well as prerecorded content.
14. Can accommodate changes without impairing the ability of the existing equipment to operate with new content or new equipment to operate with old content.
15. Can include features or accommodate changes without rendering recorded material unviewable to the extent that user has expectation of viewability.

Legal

16. Does not introduce import or export problems for the United States and other major markets.
17. Includes a technological measure which permits legal enforcement against circumvention.
18. Is licensed in accordance with the CEMA Intellectual Property Rights (IPR) policy.
19. Preserves consumer's legal rights of use, including the first sale doctrine.

When the list was completed, it was presented to the CPTWG in March 1999, and later discussed with the MPAA in April 1999.

6.2. MPAA list

After reviewing the CEMA list, the MPAA published its own list of "attributes of a security environment for distribution of protected high value content". In this list, distributed in May 1999, "Approved" means acceptable to owners of legally protected high value content exercising their individual discretion, for the purpose of protecting lawful rights. It is assumed that all content referenced in the list is legally protected, high value content. The list reflects the views of the individual member companies of the MPAA. All decisions as to whether particular technologies are acceptable, whether to invoke any particular level or form of copy protection, and other matters are for unilateral, independent determination by individual member companies.

MPAA attributes of a security environment for distribution of protected high value content:

1. The following is applicable to all linked transport, display and recording devices.
2. The same principles apply to CE and IT devices.
3. Digital bit streams are never "in the clear" (i.e., are always encrypted).
4. Bidirectional[8] digital output is allowed only with Approved digital technology protection (e.g., 5C, if Approved).
5. Unidirectional digital output is allowed only with approved digital technology protection (e.g., XCA (see Section 10), if Approved).
6. Standard definition analog video output (NTSC and PAL: 480I, 480P and 576I lines) must be protected by an Approved Analog Protection System (APS) (e.g., Macrovision) and marked by CGMS-A.[9]
7. All high definition analog video output (greater than 480P, e.g., 720 or 1080 lines) must be protected by an Approved analog protection technique. (For example, a video scrambling technique, yet to be determined and approved. A future system based on watermarking and requiring response under legislation may also be suitable.)
8. All video inputs (digital and analog) must look for and respond to an Approved watermark standard.
9. Licensed devices with recorder function must respond to copy protection flags (CGMS-A, Macrovision, and watermarks).
10. When only one copy ("copy once") is allowed, such copy must be recorded using an Approved copy protection technology in a manner that does not allow access to the content by non-participating devices and that does not allow further copying.
11. Content providers should be granted express third-party beneficiary rights to enforce licenses.
12. Specific devices should accommodate Approved revocation and renewability mechanisms. Content providers shall have the right to invoke revocation/renewal.

7. DVD protection

7.1. DVD video

The first problem addressed by CPTWG was the protection of content on DVD Video discs developed by the DVD Consortium (now known as the DVD Forum). The DVD Consortium was started as an ad hoc group in December 1995 to promote a single format for a large capacity disc, now known as DVD. The founding members were Hitachi, MEI, Mitsubishi, Philips, Pioneer, Sony, Thomson, Time Warner, Toshiba and Victor. With over 100 member companies today, the DVD Forum defines the specifications for DVDs. Currently, it has eight working groups: WG1: DVD Video, WG2: DVD-ROM Physical Format, WG3: DVD File System, WG4: DVD Audio, WG5: DVD-RAM Physical Format, WG6: DVD-R/RW Physical Format, WG9: DVD Copy Protection, WG10: DVD Professional Use.

Several proposals were studied by the DVD Forum and CPTWG. After much discussion and critical review, the DVD Forum recommended the proposal developed by MEI and Toshiba to the relevant industries. Known as the CSS, the system consists of a private scrambling system with multilayer key management. Scrambling takes place at the disc manufacturing location before the discs are pressed. As shown in Fig. 4, the CSS-protected

[8] Comunication is allowed in either direction across the interface.

[9] Copy Generation Management System – Analog: A system for encoding copy control information in transmissions and prerecorded copies of content in analog format.

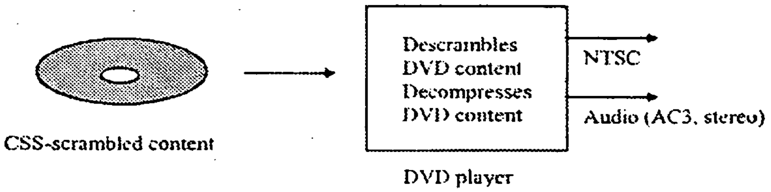

Fig. 4. CSS on a DVD player.

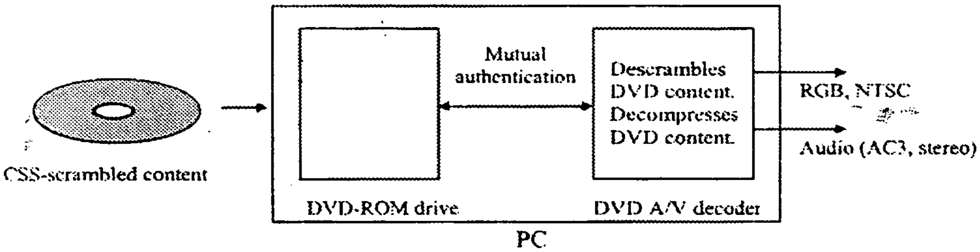

Fig. 5. CSS on a PC system.

content is descrambled during playback on a DVD player. The CSS has been very much in the news lately because a group of computer hackers has successfully attacked CSS [26]. Note that the first generation players are allowed to have NTSC (analog) output only. An analog protection system (APS) developed by Macrovision results in degradation in unauthorized copies made on VHS recorders.

Fig. 5 shows the additional element needed in CSS for implementation on a PC system. The DVD drive and the PC participate in mutual authentication before the scrambled content is sent to the descrambler. This allows each party to check if the other participant is authorized to handle CSS scrambled content.

The DVD Copy Control Association (CCA) is the entity created to license the CSS technology. The CSS Specifications are provided for each licensee to have access to the appropriate information for implementation. It includes two sections: procedural and technical. The procedural section provides the terms and conditions of the use of CSS specifications, while the technical section, designated specifically for particular membership categories, describes the system components.

7.2. DVD audio

The experience gained in DVD Video protection has helped considerably in determining an architecture for protecting prerecorded DVD Audio discs. An important factor taken into consideration for this architecture was the existence of the compact disc (CD), the first generation of digital audio format. It was argued that since a large population of CD players were still in the field, the consumers would most likely desire to have copies on recordable CD media during the transition period.

With input from the major recording studios, four companies (IBM, Intel, MEI and Toshiba) proposed a framework where watermarking and encryption are the primary technologies for preventing unauthorized playback or recording. The DVD Audio copy protection framework, which allows personal copies when authorized by content owners, is defined by the following rules:

- Devices need to have a license to descramble and to detect watermarks.
- Copying is limited to one per recorder unless more copies are authorized.
- Authorized copies must be scrambled to prevent further copies (Unprotected copies are

Table 1
Permissible CCI parameter settings

C	Specifies the number of, or other conditions for, copies authorized per recorder N: Number of copies $N = 1$ (default value) One generation No more copies No copy control
Q	Specifies the maximum sound quality of the permitted recording CD-Audio quality (default value) 2-channel full quality Multi-channel full quality
R	Indicates the authorization status for copies of each element of related content Authorized Unauthorized
T	Provides optional access control parameters Values downloaded to the DVD Audio player from the Internet may override the CCI on the Audio disc

allowed on legacy media with restricted sound quality).

- Copying for personal use is allowed at CD-Audio sound quality (Additional copies with different characteristics may be authorized by selecting different values of CCI parameters).
- The CCI parameter values must be sent securely to a licensed recording device together with scrambled content.
- Content in unscrambled digital or analog form can be sent to a licensed recorder with specific values of C and Q parameters (see below) embedded in the audio watermark.
- All outputs of DVD-Audio content except IEC-958 and analog from licensed DVD devices must be scrambled by an approved system.
- The robustness of implementation must be similar to that of CSS.

The CCI parameters, namely C, Q, R and T, allow the content owners to specify on a track by track basis the conditions for copying. Their definition and a set of permissible values that have to be supported by playback and recording devices are given in Table 1.

The copy protection framework needs the support of three systems:

1. A scrambling system for prerecorded DVD Audio discs,
2. A watermarking system for embedding CCI in the content,
3. A system for creating secure authorized copies.

Work is in progress to develop these component technologies. Specifications of Copy Protection for Pre-recorded Media (CPPM), an audio watermarking system, and CPRM (for authorized copies, see Section 7.3) are being finalized.

7.3. *Recordable DVDs (RAM/R/RW)*

The DVD Forum WG9, the working group addressing copy protection, is in the process of determining the components of the security architecture for recordables DVDs. A summary of the work is given in Table 2.

Developed by IBM, Intel, MEI and Toshiba, the proposal known as Content Protection for Recordable Media (CPRM) provides some of the components given in Table 2. Although the CPRM technology presently addresses only one DVD physical format (DVD-RAM 4.7 GB) and one application format (video recording), other physical and application formats will be considered in future revisions. The principal elements of CPRM include a private key management system and disc type recognition.

As noted earlier, the first generation DVD players were limited to have analog output only. There was not an immediate need to protect a digital stream leaving a DVD player. In home networks, however, there will be several devices (including newer generation of DVD players) with digital interfaces that need to be protected.

7.4 Historical look at DVD protection

Fig. 6 depicts three systems needed to protect DVD content in home networks. The CSS scrambles the content before it is recorded on a DVD ROM. The first generation DVD player outputs an NTSC signal after decryption and MPEG decoding. If the DVD player has an IEEE 1394 interface, the output should be protected by a second system (labeled X in Fig. 6, e.g. 5C) that performs re-encryption. Being a compliant device, the receiving unit (e.g. a digital television) has the descrambling engine and the keys for recovering the video signal. The third system (labeled Y in Fig. 6, e.g. CPRM) is needed for protecting the DVD content that was initially encrypted by CSS, and re-encrypted by X for transmission across the 1394 interface.

Table 2
Components of the copy protection architecture for recordable DVDs

Component	Decision
Disc type recognition	Will be implemented
CCI	Will be implemented
Watermark	Will be implemented
Secure transmission	Will be implemented
Encryption	Will be implemented
Compliance mark	Under discussion
Ticket	Under discussion – used by a particular watermarking technology
Authentication	Being studied for the PC environment
Unique disc ID	Under discussion

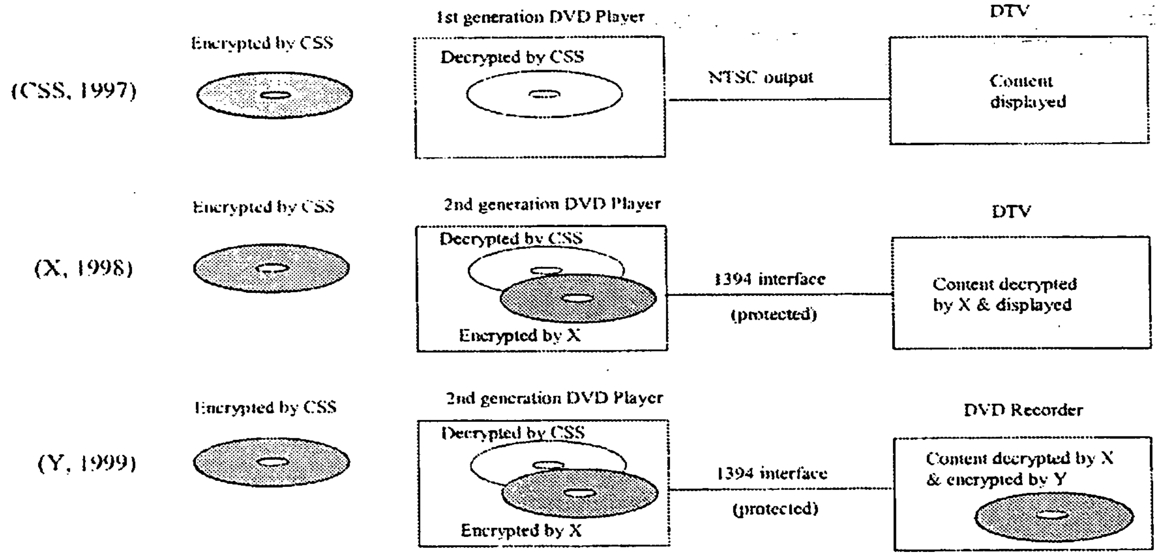

Fig. 6. Three copy protection systems for DVD protection.

7.5. Watermarking as a requirement in the CSS license

The CSS license includes the future use of a video watermarking technology for playback and recording control. The DVD CCA therefore needs to choose a watermarking technology as part of the license. The Watermark Review Panel (WaRP) was formed in December 1998 to assist CCA in evaluating the proposals. It had ten members representing the CE, IT and motion picture industries.

The seven video watermarking proposals submitted to DHSG were merged to form two groups: Galaxy (Hitachi, IBM, NEC, Pioneer and Sony) and Millennium (Digimarc, Macrovision and Philips) [2]. The key criteria used in testing these two candidates in the summer of 1999 were visibility, survivability, false positive rate, piracy, cost generational control for one copy, and licensing terms and conditions. According to the reports presented at the CPTWG meetings, Galaxy and Millennium performed similarly in the tests. A major architectural difference between the two is the scheme used for generational control [3]. Galaxy inserts a new watermark in the authorized copy, whereas Millennium processes a "ticket" (auxiliary data) attached to the content. In a recent announcement, Millennium stated that they would also provide a remarking scheme for copies. The DVD CCA has not made a decision yet.

8. Link protection

Another piece of the copy protection problem that must be solved is the protection of links between devices. It is important to note that home networks and their links are very heterogeneous. Many different systems for interconnection exist, and more are being added every year. Some examples are: 10baseT, 100baseT, HPNA,[10] IEEE 1394, baseband analog, digital visual interface (DVI),[11] various RF LAN standards, USB, IDE, AGP, NRSS and VSB-remodulation. These protocols have different characteristics (one-way versus two-way, latency, bandwidth, out-of-band control) which can render link protection designs infeasible for one or many interconnect technologies.

8.1. IEEE 1394 interface protection

The Digital Transmission Content Protection (DTCP) specification was jointly developed by Hitachi, Intel, MEI, Sony and Toshiba [4]. It defines a cryptographic protocol for protecting audio/video entertainment content from unauthorized copying, intercepting, and tampering as it traverses digital transmission mechanisms such as a serial bus that conforms to the IEEE 1394 standard. The use of this specification, and the intellectual property and cryptographic information required to implement it, are subject of a license. The Digital Transmission Licensing Administrator (DTLA) is responsible for establishing and administering the system described in the specification. The DTCP system addresses the three DTDG layers in the following way.

8.1.1. CCI layer

The CCI can be carried in two ways: Encryption Mode Indicator (EMI) and embedded CCI. The most significant bits of the synch field of the isochronous packet header are used for encoding the (EMI) bits as follows:

11: copy-never,
10: copy-one-generation,
01: no-more-copies,
00: copy-free.

CCI can also be embedded in the content stream (to be recognized by format-cognizant devices).

8.1.2. Authentication and key exchange layer

Two authentication levels are provided: full and restricted. Full authentication can be used with all types of content protected by the system. Restricted authentication is applicable for the protection of "copy-one-generation" and "no-more-copies" content only.

8.1.3. Content encryption layer

The M6 [29] cipher is defined as the baseline cipher, i.e., the cipher that must be supported by all compliant devices for interoperability. It is

[10] http://www.homepna.com/
[11] http://www.ddwg.org/

a symmetric-key block cipher based on permutation and substitution. Other ciphers such as the Data Encryption Standard (DES) [29] and Modified Blowfish [29] can also be supported.

As a result of a request from the content providers, a fourth layer has been added to allow system renewability.

8.1.4. System renewability layer

Since the security of the DTCP system relies on the secrets embedded in devices, it is not possible to renew the system by replacing the secrets. Renewability is therefore implemented using the concept of revocation. A Certificate Revocation List (CRL) is a list of device IDs identifying the devices with compromised security [4]. The DTLA generates and distributes such lists in System Renewability Messages (SRMs). Devices that support full authentication receive and store SRMs for device revocation. SRMs are updated via new content or new services in a number of ways. Some alternatives are other compliant devices with newer lists, prerecorded content media, and compliant devices with external communication capability (e.g. Internet, cable or satellite connections).

9. CEMA and copy protection

9.1. National Renewable Security Standard (NRSS)

The NRSS architecture was developed by CEMA partly in response to the Telecommunications Act of 1996. It provides a means for renewable security to be employed with digital consumer electronics devices such as digital television receivers and digital VCRs. Renewable security encompasses upgradeable, extensible, removable and replaceable security, allowing the security functionality to be separated from navigational devices. Simply stated, NRSS allows for the security system to be replaced if it has been hacked. This will be accomplished by "smart card" devices connected to consumer electronic devices.

The NRSS provides two physical designs, known as Part A and Part B. Part A defines a removable and renewable security element that is an extension of the ISO-7816 standard [22]. Part B defines a removable and renewable security element based on the PCMCIA ("PC Card") form factor. The common attributes allow either an NRSS-A or NRSS-B device to provide security for applications involving pay and subscription cable or satellite television services, telephony, and all forms of electronic commerce.

The main differences between NRSS-A and NRSS-B devices are the range of capabilities and the capacity for extension. The NRSS-A interface is limited to 8 electrical contacts using serial communication, whereas the NRSS-B interface uses 68 electrical contacts and parallel communication. In general, the NRSS-A device could be smaller and less costly, while the NRSS-B device could be more robust and extensible.

9.2. Interface protection

CEMA has standardized four interfaces for device interconnection: IEEE 1394 interface, RF Remodulator interface, NRSS interface, and analog component video interface.[12]

1. *EIA-775*: This standard [15] defines a specification for a baseband digital interface to a digital television. It is based on the IEEE 1394 Standard for High Performance Serial Bus [32].
2. *EIA-762* and *EIA-761*: These standards [16,17] define minimum specifications for a one-way data path utilizing an 8 vestigial sideband (VSB) or a 16 VSB remodulator in compliance with ATSC Standard A/53 Annex D [1].
3. *EIA-679*: This standard [12] defines a specification for a national renewable security standard. It provides an architecture to allow the conditional access functionality to be detached from consumer electronics devices.
4. *EIA-770.2* and *EIA-770.3*: These standards [13,14] define the specifications for standard definition and high definition analog component video interfaces, respectively.

Several CEMA working groups have worked on the protection of these interfaces. A summary of

[12] EIA Standards are available at http://www.eia.org for a nominal fee.

Table 3
Working groups for interface protection

Working Group	Interface	Work done
R4.8 WG2	IEEE 1394 and RF Remod	Issued a CFI on 4 November 1998. Gathered information on 5 proposals: 5C, MRJ Technology Solutions, NDS, Philips and Thomson/Zenith. Published a report [28] summarizing the proposals
R4.8 WG5	Analog component video	Issued a CFI on 2 March 1999. Gathered information on 5 proposals: C-Cube, Galaxy, Macrovision, Philips and Echostar. Published a report [5] summarizing the proposals
CEMA/NCTA JEC, NRSS Subcommittee WG2	NRSS	Defined a framework [12] for protecting the content across the NRSS interface. Five copy protection systems, all numbered for identification, support the common framework: No.1 Thomson, No.2 OpenCable, No.3 NDS, No.4 5C and No.5 Philips

this work is given in Table 3. R4 is the Video Systems Committee within CEMA. R4.8, a subcommittee reporting to R4, is responsible for all digital interfaces including their protection. The Joint Engineering Committee (JEC) was formed by CEMA and NCTA[13] to work on technical issues of common interest.

10. Global architectures for copy protection

As mentioned in Section 2, two distinct approaches have been proposed for copy protection:
(a) integration of specific solutions,
(b) a global solution.

10.1. CPSA

The Copy Protection System Architecture (CPSA) presented by IBM, Intel, MEI and Toshiba is an example of the first category. In CPSA, the original secure source is either pre-recorded DVD or electronic distribution. The content, audio or video, is protected by a group of component technologies including CSS (for video), CPPM (for audio), CPRM, DTCP, and audio and video watermarking.

10.2. XCA

A representative example of the second category is the global architecture proposed by Thomson and Zenith. The XCA Copy Protection System Specification defines a system for providing local security of audio and video content during transmission and storage in digital home networks. This task is accomplished by mapping the three basic controls, namely, "playback control", "record control" and "one-generational control" into "viewing control". Under the XCA system, content of economic value is always scrambled – either under the control and responsibility of the distributor or within the confines of the consumer's home network. XCA allows recording of XCA protected content in all conditions. Authorized copies are processed for descrambling and viewing only in licensed devices.

XCA has been developed for use with one-way and two-way digital interfaces. It is primarily

[13] National Cable Television Association (http://www.ncta.com/.)

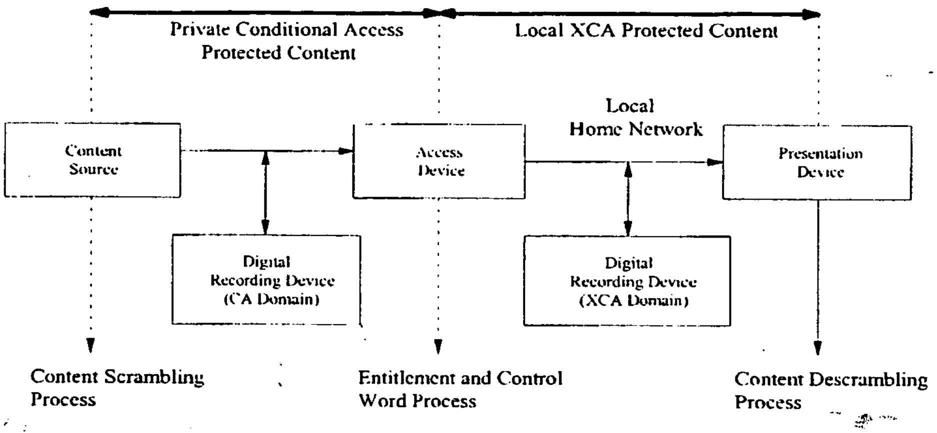
Private Conditional Access Protected Content
Local XCA Protected Content
Local Home Network
Content Source
Access Device
Presentation Device
Digital Recording Device (CA Domain)
Digital Recording Device (XCA Domain)
Content Scrambling Process
Entitlement and Control Word Process
Content Descrambling Process

Fig. 7. XCA system model.

a replaceable copy protection system to be used with renewable security devices such as smart cards.

There are three areas of technical compliance in the XCA specification:

- functional compliance of device elements,
- compliance of bit streams at the NRSS interface,
- compliance of bit streams at the level of XCA Presentation Device interconnection.

The XCA Licensing Authority is the entity responsible for administering the copy protection system. An XCA consumer electronics (CE) Device is a device that may perform either or both of the following, optionally in conjunction with a renewable security device:

- Creation of XCA protected bit streams from non-XCA protected programs,
- Descramble portions of XCA protected bit streams.

Two XCA CE devices and two removable security devices have been defined with specific functionalities. These normative device types are:

1. *Access device*: creates XCA protected content, either alone or in conjunction with a renewable security device,
2. *Presentation device*: descrambles XCA protected content, either alone or in conjunction with a renewable security device,
3. *Converter card*: a renewable security device that can create XCA protected content from private Conditional Access (CA) protected content,
4. *Terminal card*: a renewable security device that can descramble XCA protected content. Its output is compatible with the XCA NRSS interface protection system.

A digital recording device is a device that is able to store or playback XCA protected bit streams, but is unable to create or descramble XCA protected bit streams. Devices that perform digital recording or playback in combination with XCA creation or XCA descrambling shall be classified as an XCA CE Device.

The block diagram in Fig. 7 shows the basic XCA system architecture. In principle, XCA concerns itself with the protection of "after" purchase content in the home. The local access and presentation devices are the two essential elements to access, convert and display copyrighted content. The local digital recording device can be used in both CA and XCA domains for storing CA or XCA content.

10.3. Canal+ and NDS

Canal+ and NDS are two of the leading CA providers promoting a copy protection architecture similar to XCA. In this architecture, a security module coordinates all the control communications between connected compliant CE devices, and manages the viewing rights as well as recording rights associated with protected data. The security module is either a stand-alone device or a removable card embedded in a CE device in the home network. The main features of the proposed system include:

1. secure authenticated channel between the security module and the connected devices,
2. transformation of global entitlement control messages (ECMs) to personal ECMs,
3. renewable security,
4. revocation of hacked devices.

11. Secure digital music initiative

The Secure Digital Music Initiative (SDMI) is a forum that brings together the worldwide recording, consumer electronics and information technology industries to develop specifications for secure distribution of music in digital form [18]. The mission of SDMI is to enable consumers to conveniently access music, artists and recording companies to protect their intellectual property, and technology and music companies to build successful businesses in their chosen areas.

SDMI's first achievement is a specification for portable devices. The longer-term project is to complete an overall architecture for delivery of digital music in all forms.

The SDMI Portable Device Specification Part 1 (version 1.0) [18] contains implementation requirements and reference models for three functional components:

1. Applications: Perform tasks such as content import, library management, playback and rights management.
2. Portable devices and portable media: Store protected content and play it back.
3. Licensed compliant modules: Act as interfaces and translators for communications between applications and portable devices/portable media.

Compliance with the specification is voluntary. It is envisioned that the final specification will use a combination of encryption and watermarking. The subsequent parts will describe higher generation portable devices, and a generalized framework for SDMI components.

12. The US cable industry

The Telecommunications act of 1996 mandates that the US cable industry make 'navigation devices' commercially available to consumers. The Federal Communications Commission (FCC) issued a report and order in 1998 to implement this requirement. This has led to the OpenCable effort in the US. From the viewpoint of CE manufacturers, the OpenCable system has two focal points: the interface from a CE "host" to an OpenCable POD (point-of-deployment) module, and an interface from a CE device to an OpenCable settop box (which itself is probably a POD host).

OpenCable standards are created by CableLabs, which is funded by member cable-operators. CableLabs privately works with vendors of its choosing to create OpenCable standards, gain approval from their member cable operators, and then submit these standards to the Society of Cable Telecommunications Engineers (SCTE) for approval as an ANSI standard. OpenCable has defined copy protection systems for both the POD-Host interface and IEEE 1394.

13. Conclusions

The following conclusions can be drawn from our overview of copy protection in consumer electronics devices:

1. *Device interoperability is essential*: The standard interfaces developed for analog and digital signals will guarantee device interconnectivity in home networks. Nevertheless, some of the systems developed for copy protection are not compatible, and do not provide interoperability. This may present a potential problem for the consumer who may have to know what services are protected by which copy protection systems, and identify the consumer devices supporting those systems.
2. *Encryption-based technologies provide "conditional" security*: The difficulty in attacking cryptographic tools (ciphers, authentication and digital signature methods) is based on today's computational resources. With the ever increasing power of computing devices, today's secure

systems will undoubtedly no longer be robust in the future unless they are upgraded.

3. *Watermark-based technologies may require legislation*: Watermarking may require legislation with respect to whether the watermark must be detected. In the absence of a law, non-compliant devices in the market place can be used for circumvention. Watermarks may prove useful if implemented as a second line of defense complimentary to encryption.
4. *The 3 major industries (CE, IT&MP) tend to have conflicting requirements*: This is an ironical situation. The MPAA expects robust solutions (which are expensive and complex), the CE companies need the least expensive solutions, and the IT industry desires to implement everything in software.
5. *Consensus is needed*: To reach a common set of goals, the participating industries need to agree on certain legal and technical issues, opening the avenues for progress and closure.

After more than four years of work on copyrighted digital content protection, there are still some issues that have not been addressed. Some of the problems that require effective and efficient solutions in the near future are the following:

- High Definition DVD: More robust methods may be needed for this type of content.
- DVB content: Conditional access and copy protection systems are being developed in Europe.
- ATSC terrestrial TV broadcasting: A framework has been specified. Private conditional access systems will co-exist.
- Digital audio: SDMI will provide a framework for the secure distribution of digital music.
- Content distributed over the Internet: No published standard for streaming or downloaded video or other type of content.

We would like to hope that copy protection will not be a roadblock for successful deployment of digital television. The "digital world" brings many advantages, but also many interesting problems.

Acknowledgements

We would like to thank Dave Duffield of Thomson Consumer Electronics for his contributions to several sections of this work.

References

[1] Advanced Television Standards Committee (ATSC) Standard A/53, available at http://www.atsc.org.

[2] A. Bell, The dynamic digital disk, IEEE Spectrum 36 (10) (October 1999) 28–35.

[3] J.A. Bloom, I.J. Cox, T. Kalker, J-P.M.G. Linnartz, M.L. Miller, C.B.S. Traw, Copy protection for DVD video, Proc. IEEE 87 (7) (July 1999) 1267–1276.

[4] 5C Digital Transmission Content Protection, available at http://www.dtcp.com/.

[5] Compilation of Responses to Further CFI on DTV Analog Component Video Interface, available at http://www.cemacity.org/works/pubs.

[6] I. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. on Image Process. 6 (12) (December 1997) 1673–1687.

[7] D.W. Davies, W.L. Price, Security for Computer Networks, Wiley, New York, 1989.

[8] D.E.R. Denning, Cryptography and Data Security, Addison-Wesley, Reading, MA, 1983.

[9] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. on Inform. Theory 22 (6) (November 1976) 644–654.

[10] W. Diffie, M.E. Hellman, Privacy and authentication: an introduction to cryptography, Proc. IEEE 67 (3) (March 1979) 397–427.

[11] Digital Millennium Copyright Act, available at http://lcweb.loc.gov/copyright.

[12] EIA-679B National Renewable Security Standard, September 1998.

[13] EIA 770.2 Standard Definition TV Analog Component Video Interface, September 1998.

[14] EIA 770.3 High Definition TV Analog Component Video Interface, September 1998.

[15] EIA-775 DTV 1394 Interface Specification, December 1998.

[16] EIA-761 DTV Re-modulator Specification with Enhanced OSD Capability, November 1998.

[17] EIA-762 DTV Re-modulator Specification, August 1998.

[18] Guide to SDMI Portable Device Specification, available at http://www.sdmi.org.

[19] F. Hartung and M. Kutter, Multimedia watermarking techniques, Proc. IEEE, 87 (7) (July 1999) 1079–1107.

[20] M.E. Hellman, An extension of the Shannon theory approach to cryptography, IEEE Trans. Inform. Theory 23 (5) (May 1977) 289–294.

[21] Interim Report, Results of Phases I and II, Data Hiding Subgroup, Version 0.15, 16 April 1998 (available at http://www.dvcc.com/dhsg).

[22] ISO 7816-1 – Identification cards – integrated circuits cards with contacts, ISO 1987.

[23] J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, FL, 1997.

[24] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding – a survey, Proc. IEEE 87 (7) (July 1999) 1062–1078.

[25] C. P. Pfleeger, Security in Computing, Prentice-Hall, Englewood Cliffs, NJ, 1989.

[26] A. Pressman, Hollywood sues sites over DVD software, Reuters, 14 January 2000.

[27] Review and Findings of Submitted Proposals, Digital Transmission Discussion Group, Version 1.0, 11 November 1997.

[28] Review of Information Submitted in Response to the CFI, R4.8 Working Group 2, 30 July 1999.

[29] B. Schneier, Applied Cryptography, Wiley, New York, 1996.

[30] C.E. Shannon, Communication theory of secrecy systems, Bell Systems Tech. J. 28 (October 1949) 656–715.

[31] M.D. Swanson, M. Kobayashi, A.H. Tewfik, Multimedia data-embedding and watermarking technologies, Proc. IEEE 86 (6) (June 1998) 1064–1088.

[32] I.J. Wickelgren, Facts about firewire, IEEE Spectrum 34 (4) (April 1997) 19–25.

[33] R.B. Wolfgang, C.I. Podilchuk, E.J. Delp, Perceptual watermarks for digital images and video, Proc. IEEE 87 (7) (July 1999) 1108–1126.